(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 October 2001 (11.10.2001)

PCT

(10) International Publication Number
WO 01/75604 A1

(51) International Patent Classification[7]: G06F 11/30, 12/14, 15/16, 15/173

(21) International Application Number: PCT/US01/10715

(22) International Filing Date: 2 April 2001 (02.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/194,254 3 April 2000 (03.04.2000) US
09/661,500 14 September 2000 (14.09.2000) US

(71) Applicants and
(72) Inventors: **STARK, Juergen** [US/US]; 930 Vernon Avenue, Glencoe, IL 60022 (US). **GOREN, Craig** [US/US]; 1613 N. Sedgwick, Chicago, Il 60614 (US).

(74) Agent: **PINE, Jeffrey, A.**; Baniak Pine & Gannon, 150 N. Wacker Drive, Suite 1200, Chicago, IL 60606 (US).

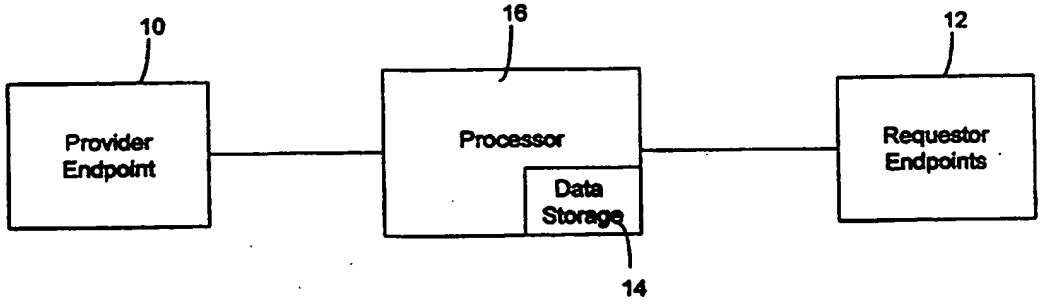
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD OF CONTROLLING ACCESS TO PERSONAL RESOURCES



(57) Abstract: The present invention relates to a semi-private security method and system that enables certain individuals (12) to access a person or provider's personal resource or endpoint (10) without the need for a shared password. The invention prevents the general public or those not having specific knowledge of the provider (10) from accessing the personal resource. The access to the resource is controlled through an identifier that relates to and can be understood from attributes or clues that only certain individuals (12) would have knowledge about.

WO 01/75604 A1

METHOD OF CONTROLLING ACCESS TO PERSONAL RESOURCES

This non-provisional application is based on the provisional patent application Serial No. 60/194,254, entitled Consumer XML Message Processing Platform, filed on April 3, 2000.

Cross reference is made to a related invention disclosed in U.S. patent application entitled Individual XML Message Processing Platform, filed concurrently, the subject matter of which is owned by the present applicants and the teachings of which are incorporated herein by reference.

Cross reference is also made to a related invention disclosed in U.S. patent application entitled Method and System for Content Driven Electronic Messaging, filed concurrently, the subject matter of which is owned by the present applicants and the teachings of which are incorporated herein by reference.

Background Of The Invention

The present invention pertains to a method of semi-private security. More particularly, the present invention pertains to a method for restricting general access to an individual (or that individual's endpoints) or restricting general access to a web site, while allowing access to certain individuals having particular knowledge about the individual or the web site. The present invention can be applied to any method or system of communication whereby all unsolicited communications are screened from the person.

Whether it is in a work environment or for personal use, users of the Internet wish to share their resources such as personal web pages, contact information, and configuration information with third parties also using the Internet. These third parties include friends, family, and business colleagues. However, for obvious reasons, users do not want to share this information with the many other users that are accessing the Internet. Moreover, most Internet users that receive electronic mail or e-mail do not want to receive unsolicited electronic messages, otherwise known as spam. Likewise, web site owners are willing to share documents or files associated with their web site,

and to share this information on a limited basis, while having some sort of security mechanism that will prevent the general public from accessing the same information.

Currently, the prior art provides only a few widely known techniques for facilitating a shared-file or shared-document environment. One of them is a type of multi-user software sold by Xerox as their Global View software product, which provides a concept of shared file drawers. Access to the drawers is either limited to a read-only basis or is limited to those users who have been given an icon to enter the drawer. A systems administrator is in charge of the icon distribution. A similar system, offered by Novell, provides a concept of a shared network drive where access is available to every file in the drive. The systems administrator controls access to the drive. A system that is applicable to web site applications, shares files or documents through hypertext or other links to a home page. These applications provide the necessary security, or access to some or all of the documents or files pertaining to that web site, by utilizing a password, which may be controlled by a web master.

Another method of controlling access to a particular resource involves cryptographic authentication algorithms that rely on public and private keys to authenticate access to the resource. One of downsides of the cryptographic authentication algorithm approach is that the keys need to be generated and then distributed to the individuals that need access to the information.

For example, if a web site is protected in such a manner, the user would have to distribute the keys to potentially hundreds of friends, family members and business associates to whom the user would like to invite access. Likewise, if all of these friends, family members and business associates had their own web sites that were also protected, they too would have to distribute similar keys to allow access to their information. Obviously, this type of distribution can be inefficient and problematic. As a result, most web sites are not protected from access by using security measures.

It can be appreciated that there exists a need for a shared data environment, which overcomes the above-mentioned drawbacks.

Summary Of The Invention

The present invention allows for protection of all types of user communication resources but eliminates the need for knowledge of a particular password or key that typically allows limited access or full entry to the resources. It is therefore primary aspect of the present invention to provide a method of controlling access to at least one personal resource of a provider, which is being requested.

The provider establishes an identifier or password and certain attributes or questions that relate to that identifier, which are commonly known only by a select group of requesters. The provider then stores the identifier and the attributes to which the identifier is to be applied. Upon receiving a request to access the provider's personal resource, the requester is asked to provide the identifier based on the attributes related to that identifier. If the correct identifier is transmitted, the requester can gain entry to the personal resource.

It is another aspect of the invention that if an incorrect identifier is transmitted, a second attribute or question is displayed. The second attribute may include a suggestion or clue related to the identifier, along with a second demand for the password. If the requester transmits the correct identifier after the second attribute is displayed, the requester can gain access to the provider's personal resources but at a different access level.

Another aspect of the invention is to generate a third attribute if the second demand for the password is responded to incorrectly. A correct response to the third attribute allows even further restricted access. Many levels can be created as long as there are further attributes or clues generated.

Another aspect of the invention is to generate an allowance message that indicates to the requester that the identifier has been successfully matched and that access to the provider devices will be provided.

Another aspect of the invention to provide a security system for use in a personal resource that is one of devices selected from the group consisting of a wired telephone, pager, wireless telephone, facsimile machine, personal digital assistant, personal web portal, email address, individual data file, and an Internet resource.

Detailed Description Of The Drawings

Figure 1 is a block diagram representing the relationship among objects within the shared environment of the present invention;

Figures 2 through 4 represent a flow chart of the method of operation of the present invention;

Figure 5 is an example of a first input demand dialogue box through which a requester may enter the resources of the provider; and

Figure 6 is an example of a second input demand dialogue box through which a requester is provided a suggestive clue to assist entering the resources of the provider.

Detailed Description Of A Preferred Embodiment

Turning now to the drawing figures, the security system of the present invention will be explained in greater detail. In order to understand the scope of the present invention, attention is first directed to Figure 1, which shows a block diagram representing the present invention. The provider, or the individual, corporation or party attempting to create and use a semi-private security system, may have a plurality of different personal resources or endpoints 10, for which protection is needed from others (requesters) attempting to contact the provider. These requesters can be family members, friends, business associates or unknown individuals. These personal resources or endpoints 10 may include, among others, facsimile machines, pagers, wired telephones, wireless telephones, personal digital assistants, personal web portals, email addresses, individual data files, or Internet resources.

It can be appreciated that with the present invention, a requester who might happen to be a telephone solicitor, may be prevented from gaining automatic access to the provider through the home telephone of the provider.

Similarly, it should be understood that a requester may be attempting to communicate with the provider through one of the same type of devices or endpoints 12 that the provider is trying to protect from access, as described above. The specific type of device 12 with which the requester is attempting to reach the provider, will control the mechanism that is used for either denying or allowing access to the provider.

Figures 2 through 4 show a flow chart for either denying or allowing the requester to access the provider. To protect his personal resources, the provider begins the process by first creating an identifier or password 40. This is done by selecting key value(s) that are generally known to a desired requester, but not known by the general public. For example, the provider may use the name of his dog as the identifier. The identifier becomes associated with each endpoint 10, and requires a prompt to be correctly entered prior to access being given to the requester to access the provider's personal resources.

The identifier 40 is stored 44 in a data storage device 14, which is linked to a processor 16. The processor 16 can be of several platforms, like a web server, a personal computer that is connected to a modem and phone line, or to a platform such as that available through an XML Messaging platform of which Centerpost is an example, and which is described in patent applications entitled Individual XML Message Processing Platform and Method And System For Content Driven Electronic Messaging, both applications filed concurrently herewith, and are incorporated herein by reference. When a requester is using a device like his email address to reach the provider, he would send an email message to the provider. The email message is received by the processor 16 as an input request signal 50. With any input request signal 50, the processor will generate a first response signal or attribute 60 which is transmitted back to the requester at the particular device he is using to try to gain access to the provider. In this case, his email address.

The first response signal 60 may comprise two parts, the first part 62 being an input demand that requires the requester to enter the provider's identifier 40 that has been stored in the data storage device 14. The second part 64 of the first response signal may be a message signal that indicates whether the identifier entered by the requester matched the identifier in storage 44.

Although there are many different ways in which to effect the request aspect of the present invention, Figure 5 illustrates one of the methods. The first response signal 60 has a message signal 64 which appears on the screen of the device 12 of the requester (in this case the computer screen displaying his email account) requesting him

to input an identifier. The response signal may, among other things, contain three keys to which the requester can enter a response.

The first key 63 is the Quit key and depression of this key will automatically disconnect the requester from the connection to the processor and end the request to access. The second key 65 is the Clear key and it is provided to allow a requester to clear an identifier input if he misspells it or if he feels he mistakenly entered the wrong identifier. Use of key 65 does not break the connection with the processor. The last key is the Enter key 67 that is used after the requester enters his identifier choice into the input area 69. Once key 67 is depressed, the input demand of the first response signal is transmitted to the device 12 of the requester. If the requester transmits the proper key value (identifier), which matches the identifier 40, then authentication is established and access is granted.

A message 71 is generated and transmitted to the requester, indicating that the identifier has been successfully matched. At that point, the processor establishes access 90 to the provider device 10 and then communication can take place between the requester and the provider.

If the requester enters an incorrect identifier 40, then a message 68 is generated and transmitted to the requester, indicating that a match was not maid and that access will be denied. A second input request signal 70 can then be generated and transmitted to the requester through device 12. The second response signal 70 would also comprise two parts, the first part 72 being a second input demand requiring the requester to again enter an identifier 40 in an attempt to match the provider's identifier. The second response signal 70 is shown in Figure 6. The second response signal also is provided with the same keys 63, 65 and 67 as the keys of the first response signal, although there are many different ways this can be accomplished.

The second part 74 of the second input request signal 70 is a message signal that provides the requester with a suggestive clue relating to the identifier 40. The input demand might be a response to a simple question that has to be correctly answered. For example, the second input demand or attribute might be related to something personal pertaining to the provider. For instance the question might be "What is my dog's

name?" and the key value would be "Spot", the name of the provider's dog. Thus, the key value is the identifier. If the proper identifier 40 is entered in response to the second input demand or attribute, then authentication is established and access is granted.

The message 76 is then generated and transmitted to the requester, indicating that the identifier has been successfully matched. At that point, the processor 16 establishes access 90 to the provider device 10 and then communication can take place between the requester and the provider.

If the identifier that was entered upon the second input demand does not match the identifier 40, then an additional message 78 is generated and transmitted to the requester, indicating that a match was not maid and that access will be denied. Of course, it is possible to add an additional level or levels of suggestive clues related to the same identifier to help a requester correctly match the indicator.

Further, different levels of access to the personal resource can be set up and then accessible depending on how many attributes must be shown to the requester before the correct identifier is transmitted. For example, if a requester enters a correct identifier on the first try, then the requester may obtain access to a certain level of the provider's personal resource 10, i.e., a particular web page or a telephone call that rings through to the provider. If a correct identifier is entered only after two attributes or questions are transmitted, the requester may only obtain access to a lower level of the resource 10, i.e., a lower-level web page (with no access to the higher level pages), or the provider's voice-mail (instead of actually reaching the provider).

The present invention obviates the need for a key to be distributed since the identifier is not a randomly generated and shared password. Rather, the identifier can relate to a personal fact or an event that certain knowledgeable individuals would know and thus be allowed access to the personal resource.

In another example, the security platform of the present invention enables a requester to send a message to one of the provider's endpoints 10 using the security method described above. However, the message would not go directly to the subscriber's intended endpoint, but instead, if the requester knew the identifier, based

on the attribute, the message would be delivered to the provider at the endpoint that the provider selected.

In this embodiment, the provider may want anyone who knows the identifier based on the attribute to be able to reach the provider at his home telephone. Thus if a requester called the provider at work, and received an attribute or question that he could answer, the requester would be transferred to the provider's home phone, whereas a requester that could not provide the correct identifier would have to leave a message on the provider's work voice-mail.

In this example, instead of the input screens shown in Figures 5 and 6, the requester would input the identifier through the alphanumerical key pad on the telephone, as is common practice with many messaging systems known today. The use of the pound sign could be used as the step necessary to initiate the transmission of the identifier.

While the invention has been described with reference to a particular embodiment, those of skill in the art will recognize modifications to structure and methods that still fall within the scope of the invention and which is described in the following claims.

WE CLAIM:

1. An apparatus for providing security for at least one personal resource of a provider, comprising:

at least one provider personal resource capable of receiving a request signal from a requester, said requester requesting access to the at least one personal resource of the provider;

a memory device for storing an identifier and at least one attribute, said attribute being related to said identifier, wherein the attribute is generated and transmitted to said requester upon receiving said request signal; and

a processor used in association with the personal resource, said processor capable of receiving a transmission from said requester and comparing said transmission to said identifier.

2. The apparatus of claim 1, wherein said processor allows access to said at least one personal resource upon receiving a transmission from said requester that is the same as said identifier.

3. The apparatus of claim 2, wherein upon receiving a transmission from said requester that is not the same as the identifier, the processor transmits a second attribute to said requester.

4. The apparatus of claim 3, wherein said requester sends said transmission via a communication device, the communication device selected from the group consisting of a wired telephone, pager, wireless telephone, facsimile machine, email address, personal digital assistant, web site.

5. The apparatus of claim 4, wherein the personal resource is one of resources selected from the group consisting of a wired telephone, pager, wireless telephone, facsimile machine, email address, personal digital assistant, web site.

6. The apparatus of claim 2, wherein the first response signal comprises an input demand and response, said input demand requiring the requester to provide an

identifier of the provider, the response being a signal indicating one of approval or disapproval to access the personal resource of the provider.

7. A method of controlling access to at least one personal resource of a provider that is being requested access thereto by a requester, comprising:

prompting the provider to establish an identifier, the identifier having a personal attribute that is commonly known only by a select group of requesters;

storing the identifier and associating at least one personal resource to which the identifier is to be applied;

receiving an input request signal from a requester to access the at least one personal resource of the provider;

generating a first response signal which informs the requester of one of approval and disapproval for access to the personal resource of the provider.

8. The method of claim 7, wherein the first response signal is comprised of an input demand and response, the input demand requiring the requester to provide an identifier of the provider, the response being a signal indicating one of approval and disapproval to access.

9. The method of claim 8, further comprising generating a second response signal if the input demand of the first response signal is a non-match, the second response signal comprising a suggestive clue related to the identifier of the provider and a second input demand to provide the identifier of the provider based upon the attribute.

10. The method of claim 9, further comprising generating a third response signal if the second input demand of the second response signal is a disapproval, the third response signal comprising a denial of access to the personal resource of the provider.

11. The method of claim 10, further comprising generating an approval message that indicates to the requester that the identifier has been successfully matched and that access to the provider devices will be provided.

12. The method of claim 8, wherein the input request signal is transmitted through a communication device, the communication device selected from the group consisting of a wired telephone, pager, wireless telephone, facsimile machine, email address, personal digital assistant, web site.

13. The method of claim 9, wherein the personal resource of the provider is a communication device selected from the group consisting of a wired telephone, pager, wireless telephone, facsimile machine, email address, personal digital assistant, web site.

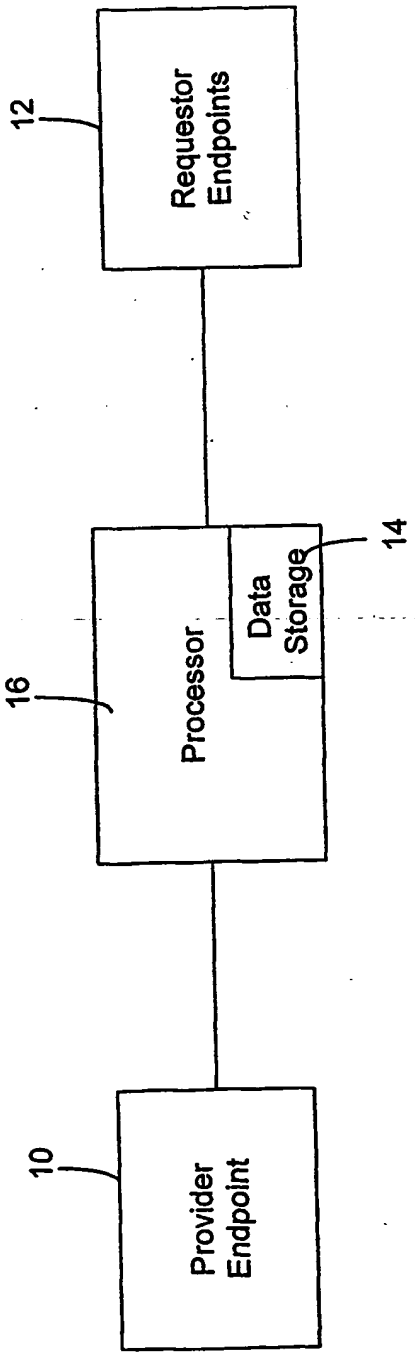

Requestor Endpoints
12
Data Storage
14
Processor
16
Provider Endpoint
10

FIGURE 1

FIGURE 2

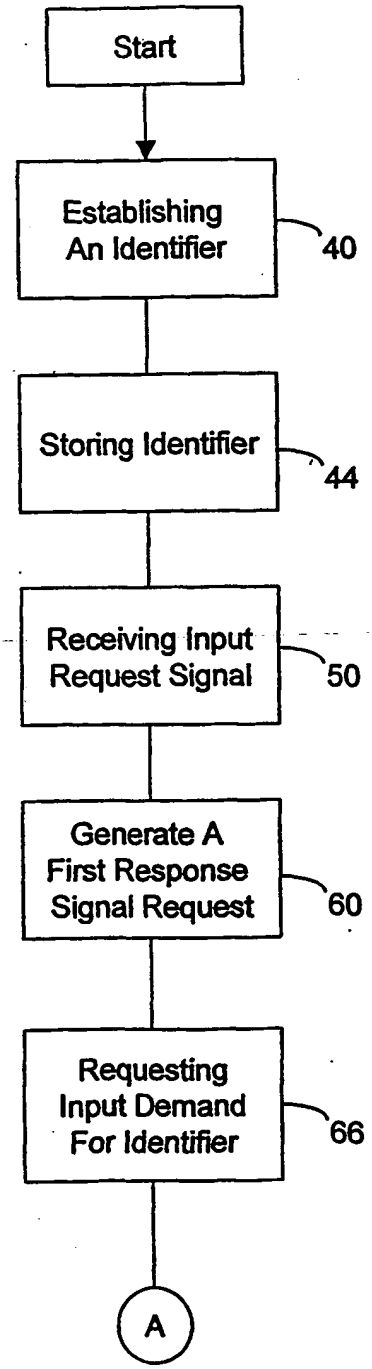

Start
Establishing An Identifier
40
Storing Identifier
44
Receiving Input Request Signal
50
Generate A First Response Signal Request
60
Requesting Input Demand For Identifier
66
A

FIGURE 3

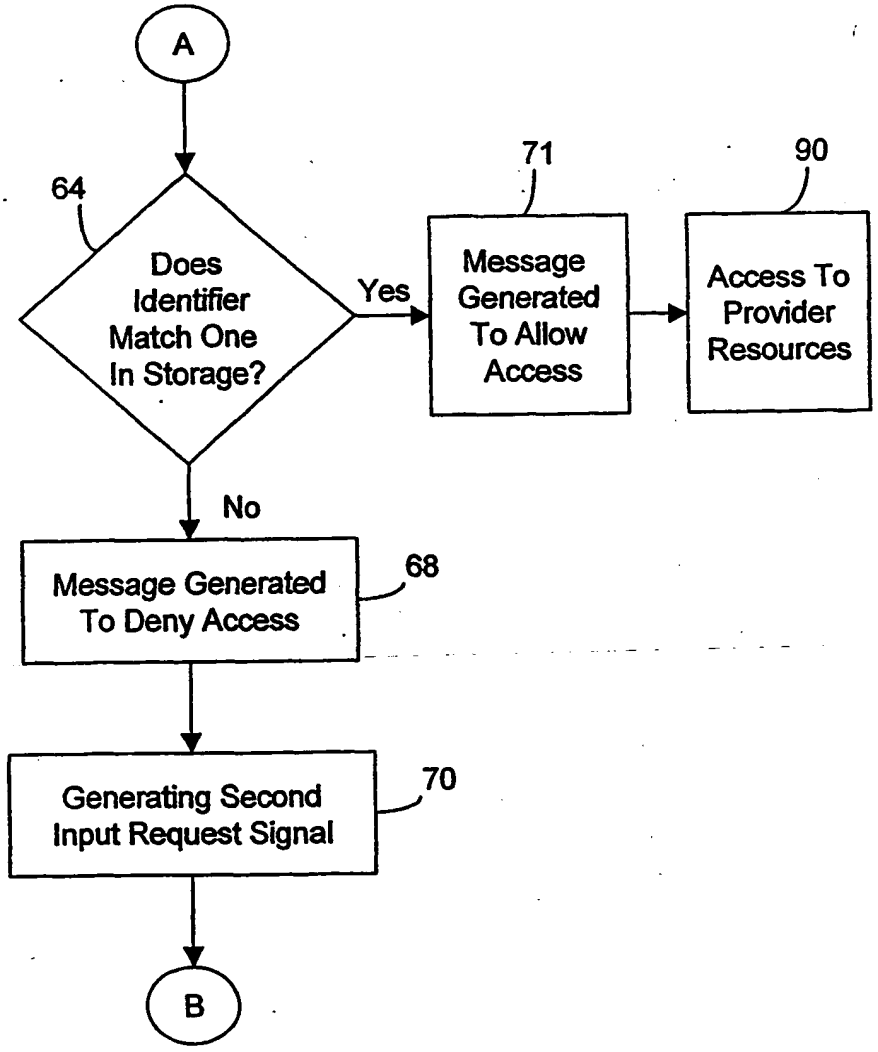
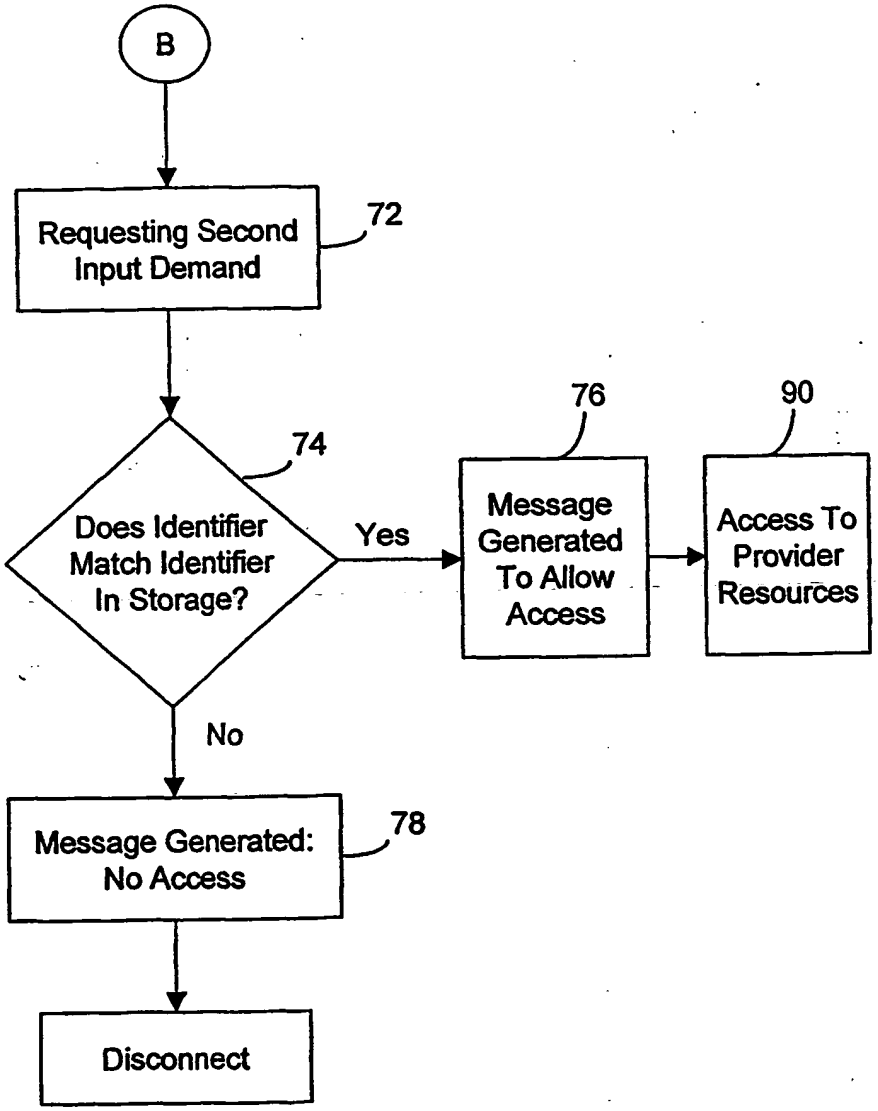

A
64
Does Identifier Match One In Storage?
Yes
71
Message Generated To Allow Access
90
Access To Provider Resources
No
Message Generated To Deny Access
68
Generating Second Input Request Signal
70
B

FIGURE 4


B
Requesting Second Input Demand
72
74
Does Identifier Match Identifier In Storage?
Yes
76
Message Generated To Allow Access
90
Access To Provider Resources
No
Message Generated: No Access
78
Disconnect

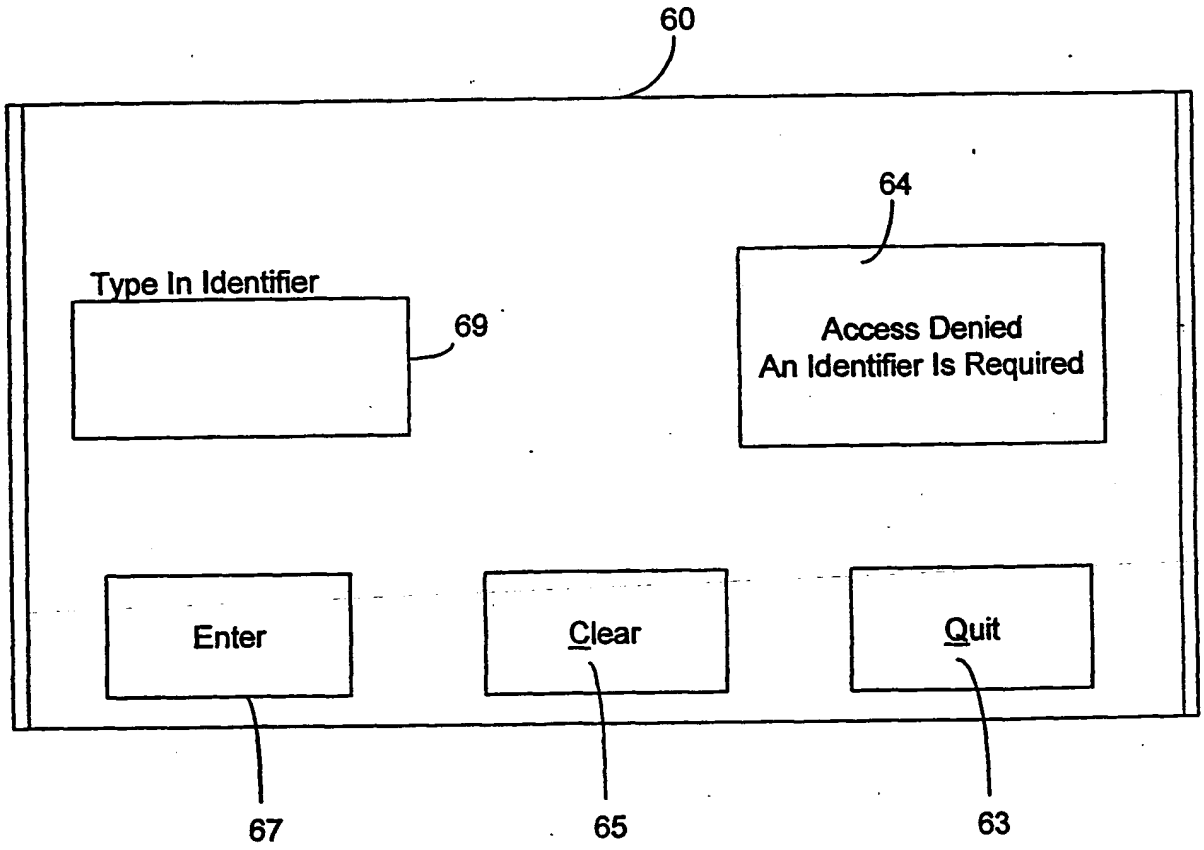

60
64
Type In Identifier
69
Access Denied
An Identifier Is Required
Enter
Clear
Quit
67
65
63

FIGURE 5

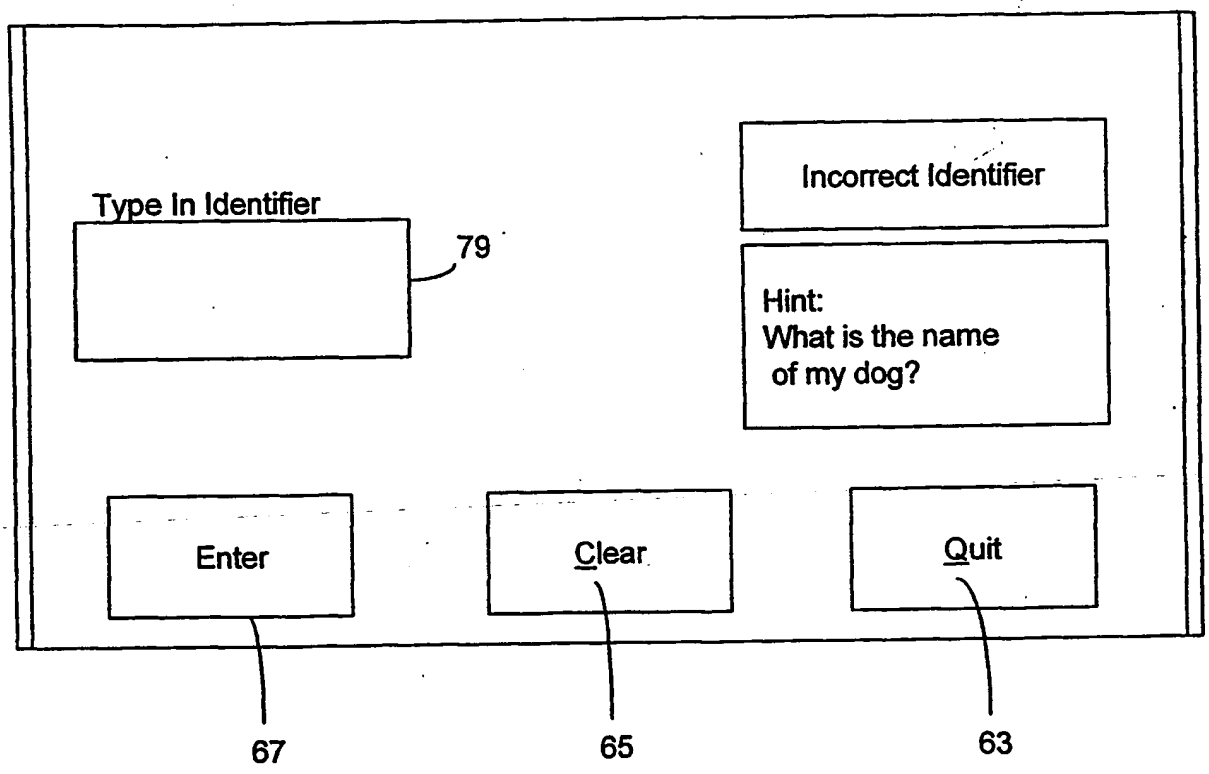

Type In Identifier
79
Incorrect Identifier
Hint:
What is the name
of my dog?
Enter
Clear
Quit
67
65
63

FIGURE 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/10715

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 11/30, 12/14, 15/16, 15/173
US CL : 713/200, 201, 202; 709/217, 218, 219, 226, 229

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201, 202; 709/217, 218, 219, 226, 229

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 792 044 A2 (SHIN ET AL) 27 AUGUST 1997, PAGES 1-17	1-13
X	US 5,708,780 A (LEVERGOOD ET AL) 13 JANUARY 1998, COL. 6, LINES 36-57, COL. 7, LINES 51-59	1,7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 27 JUNE 2001	Date of mailing of the international search report 02 AUG 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer CHRISTOPHER A REVAK Telephone No. (703) 305-9618

Form PCT/ISA/210 (second sheet) (July 1998)+

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/10715

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

BRS (FILES: USPAT, DERWENT, JPO, EPO, IBM TDBs), DIALOG (FILES: COMPSCI, ELECTRON, SOFTWARE)

search terms: challenge, challenges, challenging, challenged, hint, hints, hinted, hinting, prompt, prompts, prompting, prompted, require, required, requiring, requirement, requires, respond, response, responses, access, accesses, accessed, accessing, entry, use, usage, resource, resources, object, objects, file, files, application, applications, software